ABSTRACT

A method an apparatus for protecting a configuration data sequence from reverse engineering is provided. The configuration data sequence includes a plurality of configuration bits and is used to configure the operation of a programmable device, such as an FPGA or other reconfigurable logic. According to a method of the present invention, the configuration bits of the configuration data sequence are partially encrypted by altering some, but not all, of the bits, and subsequently storing the partially-encrypted configuration data sequence external to the programmable device. Corresponding decryption information is then stored within the programmable device, which decrypts the partially-encrypted configuration data sequence using the decryption information stored therein to thereby configure internal logic of the programmable device.